SQL インジェクション検出ツール
「iLogScanner V2.0」

ウェブサーバのアクセスログを解析して

脆弱性を狙った攻撃の検出を簡易に行うツール

取扱説明書

2008 年 11 月

目次

1. はじめに

1.1. このプログラムの目的

IPA では、Web アプリケーションに対してどれほどの攻撃を受けているのか、Web サイト管理者が簡単に状況を把握できる手段を提供していく必要があると考えています。そこで、Web サイトのアクセスログを解析することで、そのサイトへの攻撃痕跡を確認でき、一部の痕跡に関しては攻撃が成功した可能性を確認できるツール「iLogScanner」を開発しました。Web サイトへの攻撃が成功した可能性が確認された場合は、Web アプリケーションに潜む脆弱性を確認する事ができると共に、インターネットに公開しているWeb サイトがどれほど危険であるかを認知してもらい、Web サイト管理者や経営者に対して警告を発し、対策を講じるきっかけとなる事が期待できます。

1.2. 機能概要

iLogScanner は、利用者が Web ブラウザを利用して IPA の Web サイトからダウンロードし、利用者の Web ブラウザ上で実行する Java アプレット形式のプログラムです。iLogScanner は、利用者が用意した Web サーバのアクセスログファイルを解析し、Web アプリケーションへの攻撃の有無を解析結果レポートとして出力します。

1.3. 解析対象の Web アプリケーション攻撃

iLogScanner は、次の脆弱性を狙った Web アプリケーション攻撃の痕跡と攻撃が成功した可能性を検出します（2008 年 11 月現在)。

【Web アプリケーション攻撃の痕跡と攻撃が成功した可能性を検出】

- SQL インジェクション

【Web アプリケーション攻撃の痕跡を検出】

- OS コマンド・インジェクション
- ディレクトリ・トラバーサル
- クロスサイト・スクリプティング
- その他（IDS*回避を目的とした攻撃）

* IDS：侵入検知システム（Intrusion Detection System）

1.3.1　各脆弱性の説明

- 「SQL インジェクション」とは

  データベースと連携した Web アプリケーションに問合せ命令文の組み立て方法に問題があるとき、Web アプリケーションへ宛てた要求に悪意を持って細工された SQL 文を埋め込まれて（Injection）しまうと、データベースを不正に操作されてしまう問題です。これにより、データベースが不正に操作され、Web サイトは重要情報などが盗まれたり、情報が書き換えられたりといった被害を受けてしまう場合があります。

- 「OS コマンド・インジェクション」とは

  Web サーバ上の任意の OS コマンドが実行されてしまう問題です。これにより、Web サーバを不正に操作され、重要情報などが盗まれたり、攻撃の踏み台に悪用される場合があります。

- 「ディレクトリ・トラバーサル」とは、

  相対パス記法を利用して、管理者が意図していない Web サーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

- 「クロスサイト・スクリプティング」とは

  Web サイトの訪問者の入力をそのまま画面に表示する掲示板などが、悪意あるスクリプト（命令）を訪問者のブラウザに送ってしまう問題です。これにより、アンケート、掲示板、サイト内検索など、ユーザからの入力内容を Web ページに表示する Web アプリケーションで、適切なセキュリティ対策がされていない場合、悪意を持ったスクリプト（命令）を埋め込まれてしまい、Web ページを表示した訪問者のブラウザ環境でスクリプトが実行されてしまう可能性があります。その結果として、cookie などの情報の漏洩や意図しないページの参照が行われてしまいます。相対パス記法を利用して、管理者が意図していない Web サーバ上のファイルやディレクトリにアクセスされたり、アプリケーションを実行される問題です。これらにより、本来公開を意図しないファイルが読み出され、重要情報が盗まれたり、不正にアプリケーションを実行されファイルが破壊されるなどの危険があります。

- 「その他（IDS 回避を目的とした攻撃)」とは

  １６進コード、親パス等の特殊文字を使用して偽装した攻撃用文字列で攻撃が行われることによりアプリケーションの妥当性チェック機構を迂回し、SQL インジェクション、クロスサイト・スクリプティング等の攻撃を行うことを狙ったものです。また、ワームなどが悪用する Web サーバの脆弱性を突いた攻撃でも、このような特殊文字が使われます。それぞれの攻撃に応じた対策が必要になります。

脆弱性については、IPA　セキュリティセンターの「知っていますか？脆弱性（ぜいじゃくせい)」http://www.ipa.go.jp/security/vuln/vuln_contents/index.html で解説が行われていますので、ご参照ください。

2. 動作環境について

2.1. 動作環境

iLogScanner が動作する環境は、以下を想定しています。

CPU	Intel Pentium4 2.8Ghz 以上を推奨
搭載メモリ	1GB 以上を推奨
オペレーティングシステム	Microsoft Windows XP Professional SP2、SP3
Web ブラウザ	Internet Explorer 7
Java 実行環境（JRE）	Sun Microsystems 社 J2SE Runtime Environment(JRE) 5.0

JRE 5.0 ダウンロードサイトは、http://java.sun.com/j2se/1.5.0/ja/download.html になります。

その他、以下の環境においては一部動作可能であることを確認しております。

※ 以下に記載した環境での動作を保証するものではございません。オペレーティングシステム/Web ブラウザ/JRE のバージョン、利用者環境等の違いにより、動作が異なる場合もございますので、予めご了承ください（2008 年 11 月現在）。

	オペレーティングシステム（Microsoft）	Web ブラウザ	Java 実行環境（JRE）（Sun Microsystems）	動作
1	Microsoft Windows 2000 Professional SP4	Internet Explorer 6	JRE 5.0	○
2			JRE 6.0	○
3		FireFox 3	JRE 5.0	○
4			JRE 6.0	○
5	Microsoft Windows XP Professional SP3	Internet Explorer 6	JRE 5.0	○
6			JRE 6.0	○
7		Internet Explorer 7	JRE 6.0	○
8		FireFox 3	JRE 5.0	○
9			JRE 6.0	○
10	Microsoft Windows Vista Business	Internet Explorer 7	JRE 5.0	×
11			JRE 6.0	×
12		FireFox 3	JRE 5.0	○
13			JRE 6.0	○
14	Linux(CentOS 5)	FireFox 3	JRE 5.0	△
15			JRE 6.0	△

○：正常動作する　△：一部を除き正常動作する　×：正常動作しない

【補足事項】

＜Windows Vista について＞

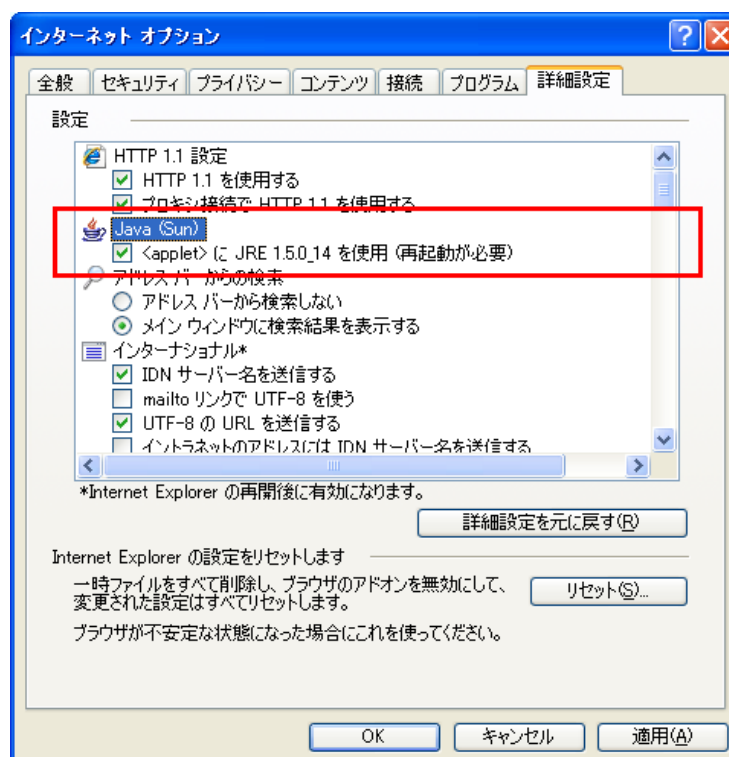
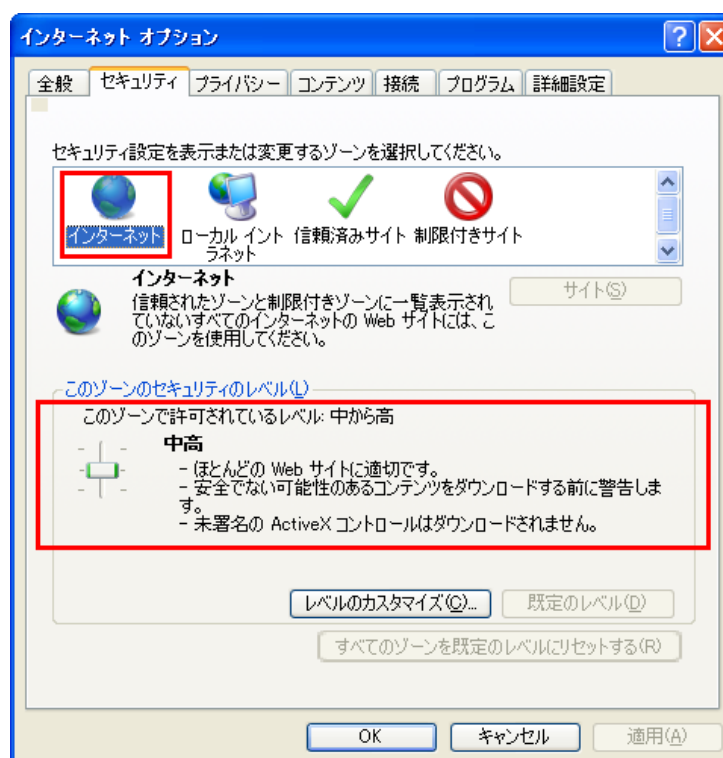
Windows Vista + IE7 では初期設定で「保護モード」が有効となっている為、iLogScanner を正常に動作させることができません。「保護モード」を無効にすると、ブラウザを悪用する不正なソフト（ウイルス、スパイウェア）などの動きを抑えることができなくなってしまいますので、セキュリティの観点から Windows Vista + IE7 上での実行は推奨しておりません。

＜Linux（CentOS 5）の動作について＞

Linux 上で FireFox3 を使用しツールを実行したところ、正常に解析処理は行われますが、ユーザが親画面（解析開始画面）を操作することが出来てしまうという現象がみられました。親画面の中ではアプレット部分を操作することはできないようにしておりますが、その他（HTML 部分、ツールバー等）は操作が行える為、画面遷移をしたりブラウザを閉じたりすることができます。この場合、当ツールは強制終了されますのでご了承ください。

2.2. Web ブラウザの設定

Java アプレットである iLogScanner を実行するために、Web ブラウザ（Internet Explorer 7）が次の設定になっていることを確認してください。設定を変更する場合は、利用終了後に既存の設定に戻せるように、現在の設定をメモしておき、利用終了後に設定を既存の値に変更してください。また、設定を変更した場合は、Internet Explorer 7 を再起動して設定を反映させる必要があります。

(1) Internet Explorer 7 のメニューから「ツール」->「インターネットオプション」を開き、「詳細設定」タブの Java の設定項目にチェックが入っていることを確認してください（Sun Microsystems 社 J2SE Runtime Environment(JRE) をインストールすると初期設定でチェックが入っています）。J2SE Runtime Environment(JRE) 5.0 Update 14 がインストールされている場合は、次の画像のようになります。

(2) 「インターネットオプション」の「セキュリティ」タブを開き、『インターネット』ゾーンを選び「このゾーンのセキュリティのレベル」が『中高（既定のレベル)』になっていることを確認してください（Internet Explorer 7 では、インターネットゾーンのセキュリティレベルの初期設定は『中高』になります)。

【補足事項】

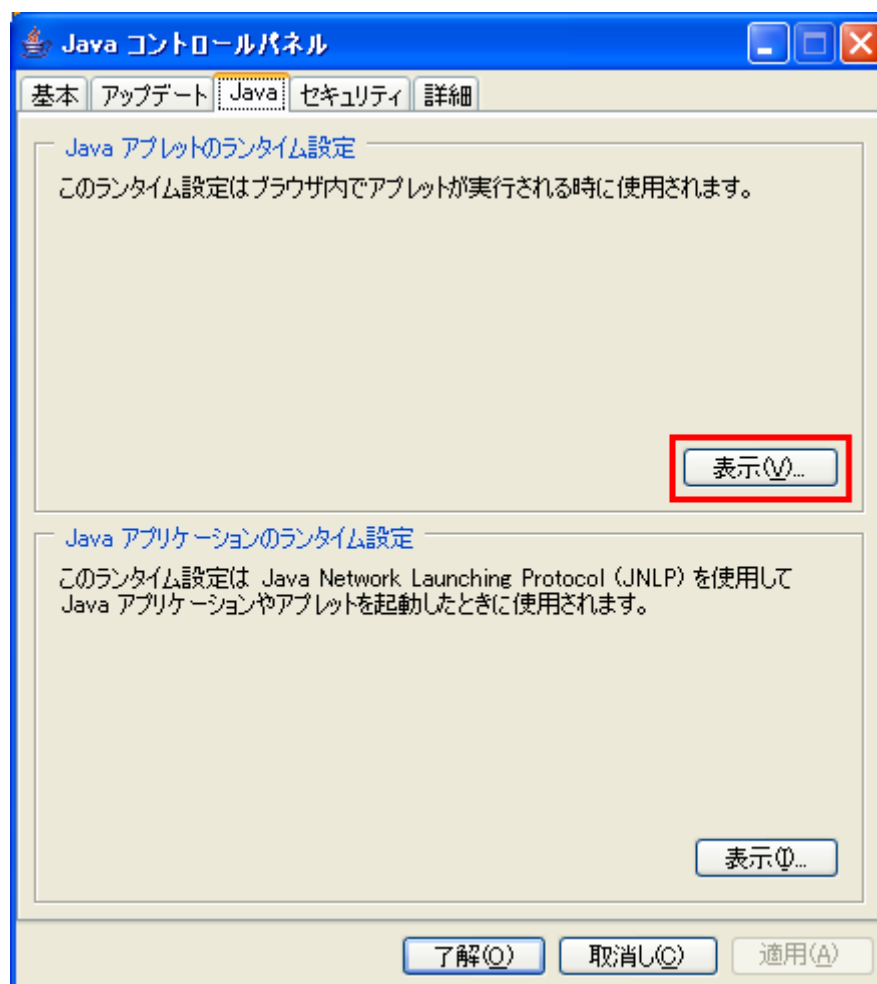
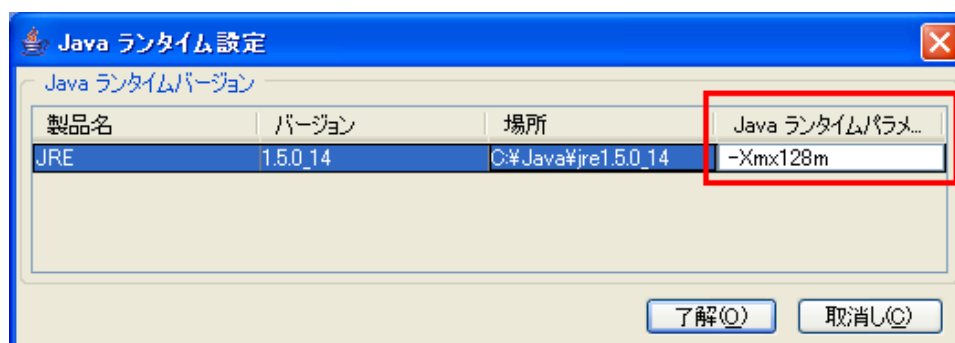
「インターネットオプション」の「セキュリティ」の設定で、セキュリティレベル『高』にしている場合、またはセキュリティレベル『高』を基本に「レベルのカスタマイズ」で任意の設定をしている場合、iLogScanner は起動しません。

「インターネットオプション」の「セキュリティ」の設定で、『インターネット』ゾーンのセキュリティレベルの設定を変更したくない場合は、『信頼済みサイト』ゾーンを選び「サイト」ボタンをクリックし、信頼済みサイトとして『https://www.ipa.go.jp』を追加した上で、「このゾーンのセキュリティのレベル」を『中高』または『中』にしてください。この設定にした場合は、iLogScanner の Web ページ接続時に『https://www.ipa.go.jp』で接続してください。

2.3.　Java の設定

Java に関する設定は、特に必要ありません。

iLogScanner 実行中に、「メモリが不足しています」という旨のエラーメッセージが表示され処理が中止された場合は、次の設定で Java が使用するメモリの最大サイズを大きくしてください（デフォルトでは 64MB です）。

(1)　コントロールパネルの「Java」より「Java　コントロールパネル」を開きます。「java」タブをクリックし、「Java アプレットのランタイム設定」の「表示」ボタンをクリックし、「Java ランタイム設定」画面を開きます。

(2)　「Java ランタイム設定」画面の「Java ランタイムパラメータ」に「-Xmx(size)m」を入力します（下記画像の例は 128MB の場合）。何も入力しない場合（デフォルト）、Java が使用するメモリの最大サイズは 64MB です。

2.4. アプレットへの署名確認

iLogScanner は電子署名された Java アプレット形式のプログラムです。このため、iLogScanner 実行時に、実行されるアプレットを信頼するかどうかのセキュリティ警告画面が表示されます。

セキュリティ警告画面では、「名前、発行者、ダウンロード元」を確認し、このアプレットが IPA から提供されていることを確認してください。詳細情報を確認する場合は、「証明書の詳細」をクリックし、発行者が信頼される機関であることと有効期限が切れていないことを確認してください。電子署名を確認後は、実行ボタンを押下して iLogScanner を実行してください。

注意：セキュリティ警告画面にて実行ボタンが押下されなかった場合、iLogScanner は動作しません。

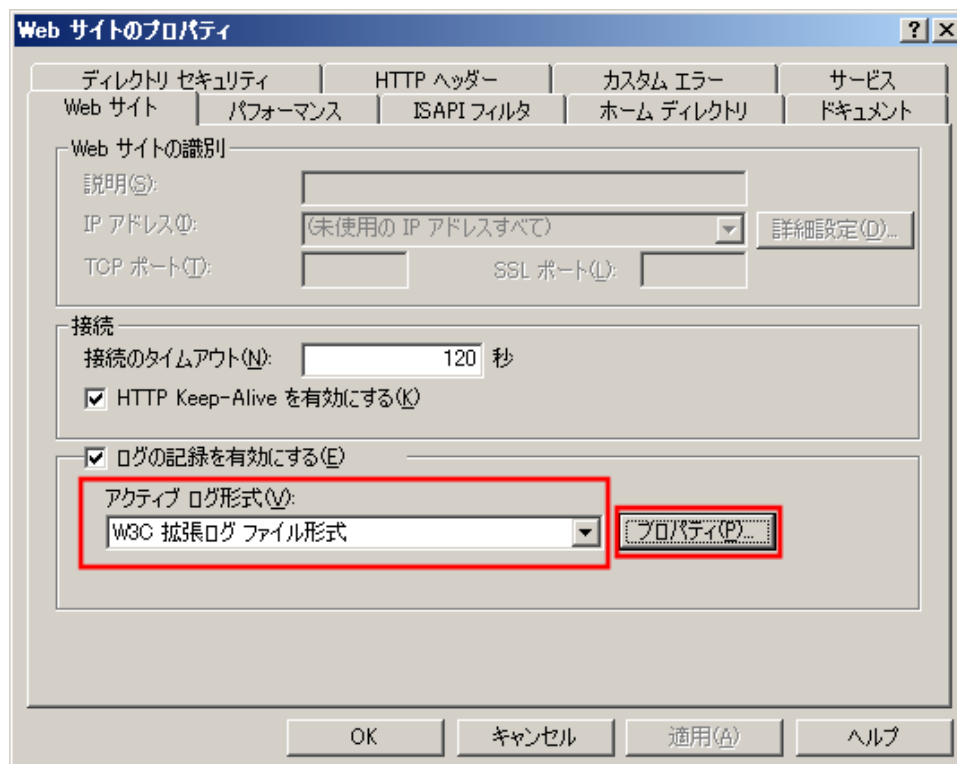
2.5. アクセスログファイル形式

iLogScanner は以下の Web サーバソフトウェアとアクセスログフォーマットに対応しております。

Web サーバソフトウェア	アクセスログフォーマット
Microsoft インターネット インフォメーション サービス(IIS 5.0、5.1、6.0、7.0)	W3C 拡張ログファイル形式
Apache HTTP Server(1.3 系、2.0 系、2.2 系)	Common Log Format

iLogScanner では、アクセスログに出力された GET メソッドのクエリ文字列を解析します。POST メソッドはアクセスログにクエリ文字列が出力されない為、POST メソッドを使用した Web アプリケーションへの攻撃痕跡の検出には対応しておりません。

(1)　W3C 拡張ログファイル形式

「インターネット インフォメーション サービス (IIS) マネージャ」の Web サイトのプロパティより、アクティブ ログ形式が「W3C 拡張ログ ファイル形式」になっている必要があります。

(画面は、IIS6.0 のプロパティになります)

また、アクティブ ログ形式のプロパティにある拡張ログ オプションにおいて次の必須項目が有効になっている必要があります。

■必須項目

日付(date)
時間(time)
クライアント IP アドレス(c-ip)
ユーザ名(cs-username)
サーバ IP アドレス(s-ip)
サーバポート(s-port)
メソッド(cs-method)
URI Stem(cs-uri-stem)
URI クエリ(cs-uri-query)
プロトコルの状態(sc-status)
ユーザエージェント(cs(User-Agent))

(2) Common Log Format

Apache HTTP Server の設定で、Common Log Format（デフォルトで定義されているニックネーム「common」形式）のアクセスログが出力されている必要があります。また、先頭からの書式が Common Log Format と同じ Combined Log Format（デフォルトで定義されているニックネーム「combined」形式）であれば解析することが可能です。

■Apache HTTP Server のアクセスログ出力設定例

```
LogFormat "%h %l %u %t ¥"%r¥" %>s %b" common
CustomLog logs/access_log common
```

■Apache HTTP Server の Common Log Format(CLF)書式

フォーマット文字列	説明
%h	リモートホスト
%l	(identd からもし提供されていれば)リモートログ名
%u	リモートユーザ
%t	リクエストを受付けた時刻。CLF の時刻の書式(標準の英語の書式)。
¥"%r¥"	リクエストの最初の行
%>s	最後のステータス
%b	レスポンスのバイト数。HTTP ヘッダは除く。CLF 書式。

3. iLogScanner 基本操作

iLogScanner は、指定したアクセスログの解析を行い、解析結果を出力します。

アクセスログ解析のために必要な項目を入力し、解析を実行すると、解析実行中画面が表示され、進捗状況を確認することができます。アクセスログ解析後は、解析結果ファイルを作成し、結果画面が表示されます。

3.1. 初期画面表示

iLogScanner トップページの下部にある「次へ」ボタンを押下後、利用規約ページへ遷移します。利用規約内容を確認し、規約に同意される方は「規約に同意する」ボタンを押して下さい。

「規約に同意する」ボタンを押した場合、iLogScanner 初期画面が表示されます。

「規約に同意しない」ボタンを押した場合、iLogScanner トップページへ遷移します。

【アクセスログファイル入力画面】

※は必須項目です

解析したいアクセスログファイルを指定してください。

アクセスログ形式： ※

解析対象アクセスログファイル名：※

参照...

解析結果の出力先ディレクトリを指定してください。

出力先ディレクトリ：※

参照...

下記ファイルの出力先ディレクトリを設定します。
出力するファイルは、実行日をもとにしたファイル名称となります。

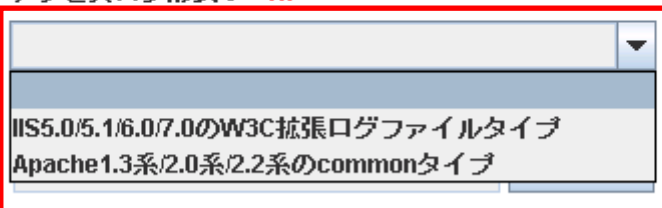
・解析結果レポートファイル(iLogScanner_年月日_時分秒.html)
・解析結果ログファイル(iLogScanner_年月日_時分秒.log)
【例】 iLogScanner_20071217_121212.html

注意：同じ名称のファイルがある場合は上書きされます。

解析開始...

3.2.　アクセスログファイルの指定

解析を行うアクセスログファイルの形式と解析対象ファイルを指定します。
アクセスログについては、「2.5　アクセスログファイル形式」を参照して下さい。

(1)　アクセスログ形式選択

▼ボタンを押してプルダウンを表示し、解析を行うアクセスログファイルのファイル形式を選択します（図はプルダウン表示状態）。

【アクセスログファイル入力画面】

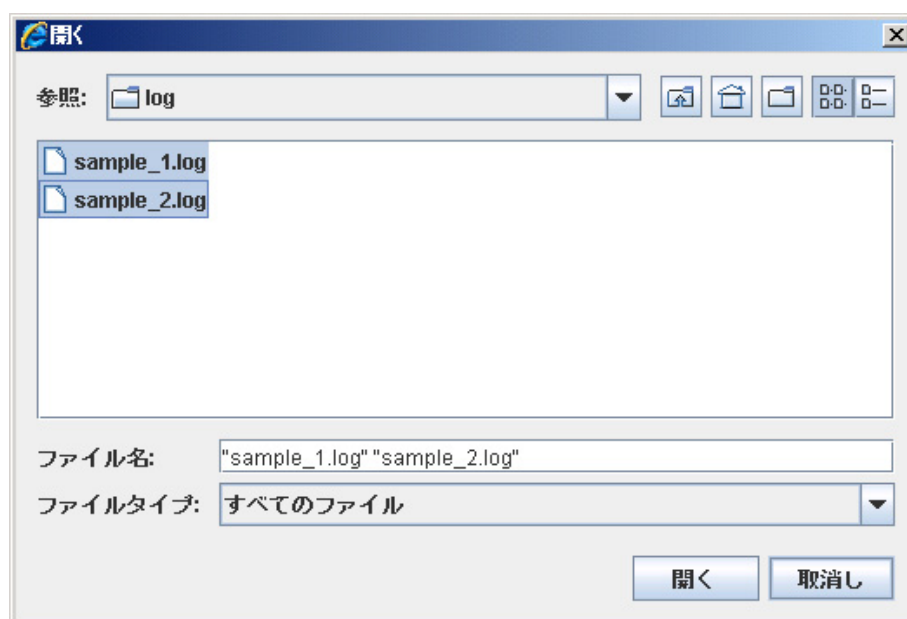
※は必須項目です
解析したいアクセスログファイルを指定してください。
アクセスログ形式：　※
IIS5.0/5.1/6.0/7.0のW3C拡張ログファイルタイプ
Apache1.3系/2.0系/2.2系のcommonタイプ

(2)　解析対象アクセスログファイル名選択

「参照」ボタンを押すと、ファイル選択画面が表示されます。

【アクセスログファイル入力画面】

※は必須項目です
解析したいアクセスログファイルを指定してください。
アクセスログ形式：　※
IIS5.0/5.1/6.0/7.0のW3C拡張ログファイルタイプ
解析対象アクセスログファイル名：※
参照...

ファイル選択画面にて解析を行うアクセスログファイル名を選択し、開くボタンを押してください。また、アクセスログファイルは複数選択することも可能です。複数選択する場合は、Shift キー(または Ctrl キー)を押しながらファイルを選択します。

3.3. 解析結果出力先ディレクトリの指定

解析結果を出力するディレクトリを指定します。参照ボタンを押すと、ディレクトリ選択画面が表示されます。ディレクトリ選択画面にて、解析結果レポートファイルと解析結果ログファイルの出力先を選択します。解析結果レポートファイル、解析結果ログファイルについては「3.6 解析結果レポート」「3.7 解析結果ログ」を参照して下さい。

エラー時に出力するエラーログもここで設定したディレクトリに出力されます。出力ディレクトリ設定前にエラーが生じた場合、出力先は実行時のカレントディレクトリになります。

3.4. 解析開始

アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリをそれぞれ設定後、解析開始ボタンを押すとアクセスログ解析が開始されます。アクセスログファイル形式、解析対象アクセスログファイル、出力先ディレクトリが全て設定されていない場合、解析は行われません。

【アクセスログファイル入力画面】

※は必須項目です

解析したいアクセスログファイルを指定してください。

アクセスログ形式： ※

IIS5.0/5.1/6.0/7.0のW3C拡張ログファイルタイプ

解析対象アクセスログファイル名： ※

sample_1.log,sample_2.log　参照...

解析結果の出力先ディレクトリを指定してください。

出力先ディレクトリ：※

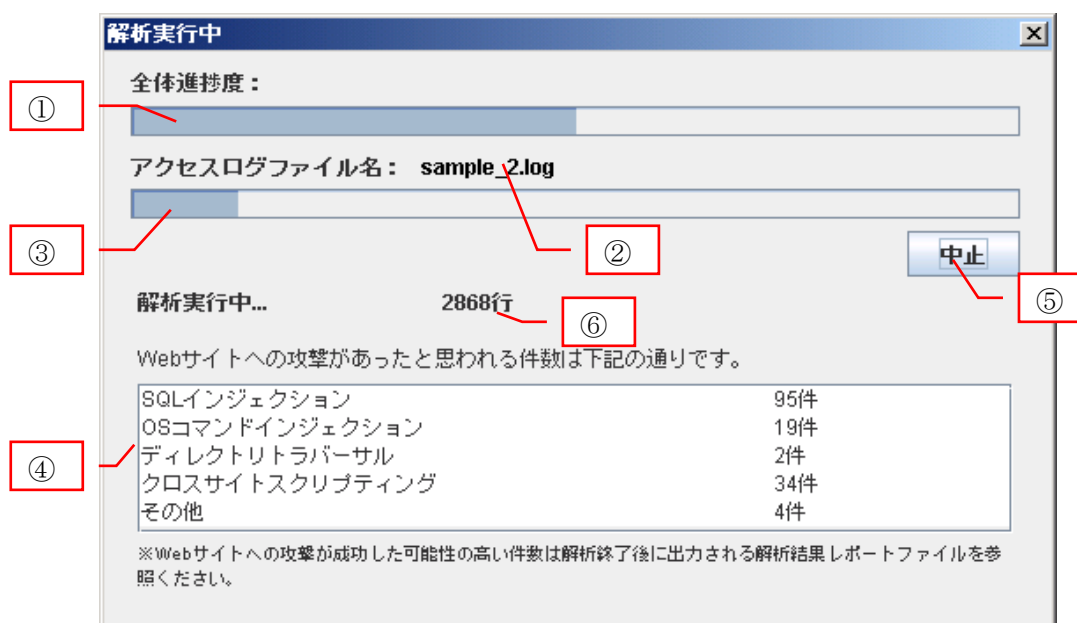
E:\log\ScanReport　参照...

下記ファイルの出力先ディレクトリを設定します。
出力するファイルは、実行日をもとにしたファイル名称となります。

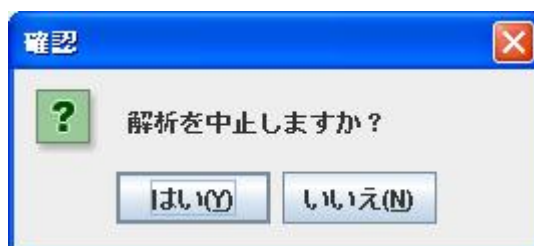
・解析結果レポートファイル(iLogScanner_年月日_時分秒.html)
・解析結果ログファイル(iLogScanner_年月日_時分秒.log)
【例】 iLogScanner_20071217_121212.html

注意：同じ名称のファイルがある場合は上書きされます。

解析開始...

アクセスログ解析が開始されると、解析中画面が表示されます。解析中画面では、アクセスログ解析の進捗情報を表示します。①は全体の解析進捗状況が表示されます。②は解析中のファイル名が表示されます。③はファイル単位の解析進捗状況が表示されます。④は、検出対象脆弱性検出数がリアルタイムで表示されます。⑤は解析中止ボタンです。解析を途中で中止したい場合、このボタンを押してください。⑥は解析対象ファイルの解析した行数が表示されます。

中止ボタンを押下した場合、確認ダイアログが表示されます。

確認ダイアログの「はい」を選択した場合、処理を中止しその時点での解析結果を出力します。

「いいえ」を選択した場合、解析実行中画面に戻ります。

3.5.　解析終了

アクセスログ解析が終了した後、結果ファイル(解析結果レポートファイル、解析結果ログファイル)を作成し、結果画面が表示されます。

【解析結果サマリ画面】

解析結果サマリ画面の①は終了メッセージ(完了/中止)が表示されます。②は攻撃痕跡の有無を示すメッセージが表示されます。③は検出対象脆弱性名と検出数が表示されます。④は結果レポートファイルのパス付ファイル名が表示されます。⑤は結果ログファイル※のパス付きファイル名が表示されます。

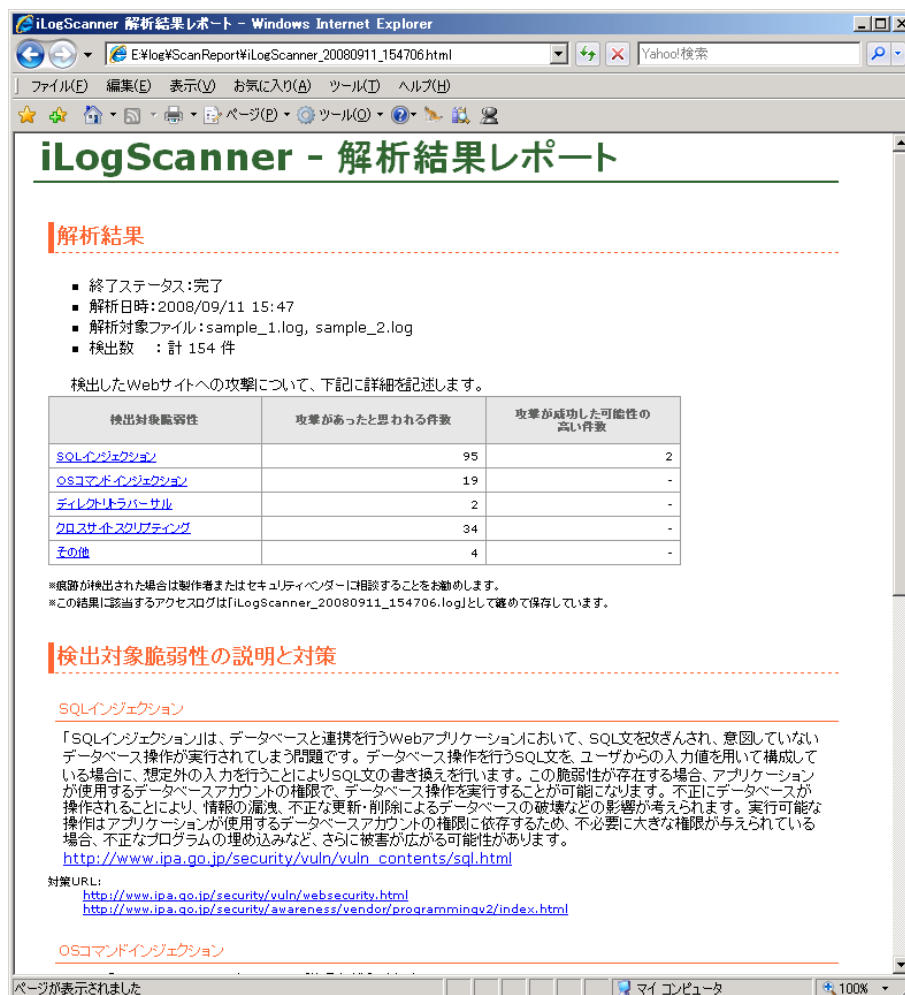
また、アクセスログ解析終了時には、解析結果レポートファイルと解析結果ログファイル※が作成されます。これらの解析結果ファイルは、アクセスログ解析前に指定されたディレクトリに出力されます。

解析結果レポートファイルには解析結果詳細情報が出力され、解析結果ログファイル※には検出したログデータが出力されます。

アクセスログ解析を中止した場合やエラーにより解析中止となった場合は、その時点までの解析結果を出力します。

※解析結果ログファイルは攻撃痕跡を検出した場合のみ出力します。

3.6.　解析結果レポート

解析結果レポートは、アクセスログ解析終了後、解析前に指定した出力先ディレクトリに出力されます。

解析結果レポートには、解析結果詳細情報と検出対象脆弱性の説明が表示されます。

解析結果情報（上段）では、終了ステータス(完了/中止)、解析日時、解析対象ファイル、検出数（攻撃痕跡の件数と攻撃が成功した可能性が高い件数)が表示されます（①は攻撃痕跡を検出した場合のみ表示)。

検出対象脆弱性（下段）では、iLogScanner が検出対象としている脆弱性についての説明が表示されます。対策の詳細については、下記サイトを参照ください。

・IPA　セキュリティセンターの「安全なウェブサイトの作り方」
　http://www.ipa.go.jp/security/vuln/websecurity.html
・IPA　セキュリティセンターの「セキュア・プログラミング講座」
　http://www.ipa.go.jp/security/awareness/vendor/programmingv2/

アクセスログ解析にて Web サイトへの攻撃痕跡が検出された場合は、製作者またはセキュリティベンダーに相談することをお勧めします。また、Web アプリケーション脆弱性が存在した場合は、脆弱性を放置せず Web アプリケーションを正しく改修して脆弱性がなくなるまで対策を施してください。

3.7. 解析結果ログ

解析結果ログファイルは、攻撃詳細が記載され、解析結果レポートと同じディレクトリに出力されます。

解析結果ログファイルの形式は以下のとおりです。

```
#解析結果ログの見方
#-------------------------------------------------------------------------------
#[ログファイル名]
#[行番号] [脆弱性種別] [攻撃が成功した可能性が高い] [該当するアクセスログ][シグネチャ対応コード]
#-------------------------------------------------------------------------------
#※ 各項目はタブ区切りになります
#※ 攻撃が成功した可能性が高い場合、「●」がつきます
#以下、解析結果ログ

sample1.log
      9  SQLインジェクション ●      2005-03-16 15:00:03 XXXXXXXXXXX XXXX

sample2.log
     11  SQLインジェクション -      2007-12-11 15:03:47 XXXXXXXXXXX XXXX
     22  SQLインジェクション -      2007-12-11 15:03:47 XXXXXXXXXXX XXXX
     23  SQLインジェクション -      2007-12-11 15:03:47 XXXXXXXXXXX XXXX
     26  SQLインジェクション -      2007-12-11 15:03:47 XXXXXXXXXXX XXXX
     47  SQLインジェクション -      2007-12-11 15:03:48 XXXXXXXXXXX XXXX
                                    ・
                                    ・
```


①は攻撃痕跡を検出したファイル名が出力されます。②は検出した行番号が出力されます。③は検出した脆弱生項目名が出力されます。④は攻撃された可能性が高い場合に「●」が出力されます。⑤は検出されたアクセスログが出力されます。⑥には内部で使用するコードが出力されます。

4. FAQ

iLogScanner に関する FAQ です。

4.1. iLogScanner とは何ですか？

「iLogScanner」は、Web サーバのアクセスログから Web アプリケーション脆弱性を狙った攻撃と思われる痕跡を検出する為のツールです。

今までは特別なスキルが必要だった Web サーバのアクセスログ解析が、「iLogScanner」を使えば誰でも簡単に行うことができ、今すぐ危険な攻撃と思われる痕跡の有無を確認することが出来ます。

攻撃と思われる痕跡の有無を確認することにより、必要なセキュリティ対策が明らかになります。

- 攻撃と思われる痕跡を全て網羅し、確実に検出するものではありません。また誤検出の場合もあります。
- iLogScanner で攻撃が検出された場合や、特に攻撃が成功した可能性が検出された場合は、ウェブサイトの開発者やセキュリティベンダーに相談されることを推奨します。
- iLogScanner は簡易ツールであり、SQL インジェクション等の攻撃のアクセスログが無ければ脆弱性を検出しません。また、実際の攻撃による脆弱性検査は行っていません。攻撃が検出されない場合でも安心せずに、ウェブサイトの脆弱性検査を行うことを推奨します。
- 解析対象アクセスログについて、検出が可能な形式がきまっております。必ず、「解析対象のアクセスログ詳細」をご確認ください。形式が異なる場合、脆弱性の検出が行われない、または脆弱性が検出されません。

Web ブラウザ上で実行する Java アプレット形式のツールとなっているので、ホームページを見ることができる環境ならば、どこでも簡単に使用することができます。

4.2. 検査結果などのデータを IPA に送信していますでしょうか？

現在は、クライアントから IPA へデータの送信は一切行っておりません。

4.3. iLogScanner は無料で使用できるのですか？

「iLogScanner」は無償で提供され、情報を一切外部に送信することが無いので、手軽にダウンロードして実行することが出来ます。

4.4. iLogScanner が検出できる Web アプリケーション攻撃の種類を教えてください。

次の脆弱性を狙った Web アプリケーション攻撃の痕跡を検出します（2008 年 11 月現在）。

1．SQL インジェクション
2．OS コマンド・インジェクション
3．ディレクトリ・トラバーサル
4．クロスサイト・スクリプティング
5．その他

- 脆弱性の概要については、「知っていますか？脆弱性（ぜいじゃくせい）[2]」を参照ください。
- 脆弱性の対策については、「安全なウェブサイトの作り方[3]」を参照ください。

4.5. iLogScanner が動作する環境を教えてください。

「iLogScanner」が動作する環境は、次を想定しています。

オペレーティングシステム	Microsoft Windows XP Professional SP3
Web ブラウザ	Internet Explorer 7
Java 実行環境(JRE)	Sun Microsystems 社 J2SE Runtime Environment(JRE) 5.0

その他、次の環境においては一部動作可能であることを確認しております。

- 次に記載した環境での動作を保証するものではございません。オペレーティングシステム/Web ブラウザ/JRE のバージョン、利用者環境等の違いにより、動作が異なる場合もございますので、予めご了承ください（2008 年 11 月現在)。

	オペレーティングシステム	Web ブラウザ	Java 実行環境(JRE※)	動作
1	Microsoft Windows 2000 Professional SP4	Internet Explorer 6	JRE 5.0	○
2			JRE 6.0	○
3		FireFox2	JRE 5.0	○
4			JRE 6.0	○
5	Microsoft Windows XP Professional SP2	Internet Explorer 6	JRE 5.0	○
6			JRE 6.0	○
7		Internet Explorer 7	JRE 6.0	○
8		FireFox2	JRE 5.0	○

[2] http://www.ipa.go.jp/security/vuln/vuln_contents/index.html
[3] http://www.ipa.go.jp/security/vuln/websecurity.html

9			JRE 6.0	○
10	Microsoft Windows Vista Business	Internet Explorer 7	JRE 5.0	×（i）
11			JRE 6.0	×（i）
12		FireFox2	JRE 5.0	○
13			JRE 6.0	○
14	Linux（CentOS 5）	FireFox2	JRE 5.0	△（ii）
15			JRE 6.0	△（ii）

○：正常動作する　　△：一部をい除き正常動作する　　×：動作しない

※ JRE：Sun Microsystems 社 J2SE Runtime Environment

i)　Windows Vista + IE7 で保護モードが有効の場合、iLogScanner は正常に動作しません。保護モードを無効にしてしまうと、ブラウザを悪用する不正なソフト（ウイルス、スパイウェア）などの動きを抑えることができなくなってしまいますので、セキュリティの観点から Windows Vista + IE7 上での実行は推奨していません。

ii)　Linux（CentOS 5） の動作について。Linux 上で FireFox 3 を使用しツールを実行したところ、正常に解析処理は行われますが、ユーザが親画面（解析開始画面）を操作することが出来てしまうという現象がみられました。親画面の中ではアプレット部分を操作することはできないようにしておりますが、その他（HTML 部分、ツールバー等）は操作が行える為、画面遷移をしたりブラウザを閉じたりすることができます。この場合、当ツールは強制終了されますのでご了承ください。

4.6.　攻撃と思われる痕跡はどのように検出しているのですか？

Web サーバのアクセスログに記録されたリクエストのクエリ文字列から、Web アプリケーションへの攻撃によく見られる文字列が存在した場合に検出しています。

それぞれの攻撃でよく見られる文字列は次のような意味のある文字列になります。

攻撃種別	文字列
SQL インジェクション	• SQL ステートメントで使用されるキーワード • データベースのシステムテーブル名 • SQL ステートメントで使用される関数 • システムストアドプロシージャ名 • システム拡張ストアドプロシージャ名

OS コマンド・インジェクション	コンピュータの基本ソフトウエアを操作するための命令文やそれらのパラメータ文
ディレクトリ・トラバーサル	ディレクトリ操作文
クロスサイト・スクリプティング	• スクリプト関数 • HTML タグ文字列 • イベントハンドラ
その他（IDS[4]回避を目的とした攻撃）	**特殊文字を使用して、偽装した文字列**

- 一般的な GET メソッドを使用した Web アプリケーションについて、リクエストのクエリ文字列から攻撃と思われる痕跡を検出しています。
- 一般的な POST メソッドを使用した Web アプリケーションについては、リクエストのクエリ文字列がアクセスログに出力されない為、攻撃と思われる痕跡を iLogScanner で検出することはできません。
- Web アプリケーションへ無差別に攻撃するような一部の攻撃は、 POST メソッドによる攻撃の場合でもリクエストのクエリ文字列がアクセスログに出力される場合がある為、iLogScanner で検出できる場合があります。
- 攻撃が成功した可能性が高いかどうかを検出することができるのは、SQL インジェクションの攻撃と思われる痕跡からのみとなります。

4.7. 攻撃が成功した可能性が高い痕跡はどのように検出しているのですか？

攻撃を受けた際、Web サーバのアクセスログに内部エラーが発生したログや攻撃成功時に記録されるログなどの、特徴的なログが記録されている場合、攻撃が成功した可能性が高い痕跡として検出しています。

- Web アプリケーションの実装や使用するサーバソフトウェアによっては、アクセスログに特徴的なログが記録されず、攻撃が成功した可能性が高い痕跡を検出できない場合もあります。
- Web サーバのアクセスログに記録された攻撃の痕跡は、攻撃を受けたことが記録として残っているのみで、攻撃を受けた結果（攻撃の成功可否）については記録されていません。このため、iLogScanner の解析だけでは、攻撃の成功／失敗について確実な判断をすることはできません。
- 攻撃が成功した可能性が高いかどうかを検出することができるのは、SQL インジェクションの攻撃と思われる痕跡からのみとなります。

[4] IDS : 侵入検知システム（Intrusion Detection System）

- 攻撃が成功した可能性が高い痕跡が検出されない場合でも、攻撃と思われる痕跡が検出された場合は製作者またはセキュリティベンダーに相談することをお勧めします。

4.8. 解析結果で攻撃があったと思われる痕跡が検出されたのですが、どうすればよいですか？

痕跡が検出された場合は、製作者またはセキュリティベンダーに相談することをお勧めします。

- なお、iLogScanner は簡易ツールであり、実際の攻撃による脆弱性検査は行っていません。攻撃が検出されない場合でも安心せずに、ウェブサイトの脆弱性検査を行うことをお勧めします。

4.9. Java アプレット画面が表示されませんが、何が原因と考えられますか？

1．JRE がインストールされていますか？

Java アプレットを動作させるためには、JRE が必要になります。Sun Microsystems 社のダウンロードサイトから、「J2SE Runtime Environment(JRE) 5.0」をダウンロードしてインストールしてください。

2．インストールされている JRE のバージョンが 5.0 より古いバージョンではないですか？

「iLogScanner」が動作する JRE のバージョンは 5.0 となります。JRE 5.0 をインストールしてください。

3．Web ブラウザのセキュリティ設定で Java アプレットが起動するように設定されていますか？

「操作手順」の「2.2.Web ブラウザの設定」を参考にして、Java アプレットが起動するように設定してください。

4.10. 実行中、「指定されたディレクトリは、存在しないか書き込み権限がありません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

解析結果の出力先として指定されたディレクトリへの書き込みが許可されていない可能性があります。ディレクトリのセキュリティ設定をご確認ください。

4.11. 実行中、「メモリが不足しています」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

解析するアクセスログファイルに 1 行が非常に大きいログがある場合、Java Plug-in でエラーが発生する場合があります。この場合、Java の起動パラメータ「-Xmx(size)m」

を指定して Java が使用するメモリの最大サイズを大きくしてください(デフォルトでは64MB です)。設定方法の例は「操作手順」の「2.3.Java の設定」をご確認ください。

4.12. 実行中、「システムエラーが発生しました」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

エラーメッセージに記載されているエラーコードをメモとしてお控えいただき、下記のお問合わせ先へご連絡ください。

4.13. 実行画面の表示で英数字以外の文字が全て"□"で表示されてしまいます。どうすればよいですか？利用環境は、Vline Linux4.2/FireFox2.0/JRE6 です。

詳細は、Tips 集に記載しております。「操作手順」の「4.Tips 集」をご確認ください。

4.14. iLogScanner が動作しません。利用環境は、WinXP/Firefox/JRE6 です。どうすればよいですか？

JRE6 のバージョンは新しいでしょうか。

JRE6 の古いバージョンにて FireFox で Java アプレットを起動した際、FireFox がハングアップする現象が確認されております。

JRE6 update6 以降にアップデートしてください。

4.15. 「SQL インジェクションによるホームページ改ざん行為」は iLogScanner で検出できるでしょうか？

「SQL インジェクションによるホームページ改ざん行為」が行われたことを検出することはできません。改ざん行為が行われた可能性が高い痕跡を検出することはできます。

4.16. 実行中、「ファイルまたはディレクトリが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

実行途中でファイルまたはディレクトリが消された可能性があります。選択したファイルまたはディレクトリを確認してください。

4.17. 実行中、「入力ファイルのログタイプ形式が不正です。」という旨のメッセージが表示され、解析処理が行われません。どうすればよいですか？

アクセスログのログタイプが異なるか、または必須項目が出力されていない可能性があります。アクセスログについての詳細は、「解析対象のアクセスログ詳細」をご確認ください。

4.18. 実行中、「当ツールを実行する許可が取消しされました。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

実行時に表示された署名確認画面でキャンセルを選択されませんでしたでしょうか。署名確認画面がキャンセルされた場合は、当ツールは実行されません。

※ツール実行時に表示された署名確認画面の署名内容を必ず確認してください。

※一度、Web ブラウザを閉じ、再度、Web ブラウザを起動をしていただく必要があります。

4.19. アクセスログの解析にはどのくらい時間がかかりますか？

それぞれ、あるサーバの 1 週間分毎のログを解析した事例を記載します。

【解析事例-1】

- 解析用アクセスログファイル

Apache1.3 系/2.0 系/2.2 系の common 形式のアクセスログファイル

Apache-1：ファイルサイズ 64MB／259K 行（攻撃検出数 0 件）
Apache-2：ファイルサイズ 61MB／253K 行（攻撃検出数 18 件）
Apache-3：ファイルサイズ 48MB／200K 行（攻撃検出数 144 件）
Apache-4：ファイルサイズ 58MB／234K 行（攻撃検出数 160 件）

- iLogScanner の動作環境

CPU：	Intel Core2 CPU 6600 2.4GHz
Memory：	2GB
OS：	Microsoft Windows XP Professional SP2
Java ランタイムパラメータ：	最大ヒープサイズ 256MB（-Xmx256m）

- 解析時間

Apache-1：12 分
Apache-2：13 分
Apache-3：10 分
Apache-4：12 分

【解析事例-2】

- 解析用アクセスログファイル

Apache1.3 系/2.0 系/2.2 系の common 形式のアクセスログファイル

Apache-5：ファイルサイズ 126MB／494K 行

Apache-6：ファイルサイズ 160MB／632K 行

- iLogScanner の動作環境

CPU：	Intel Core2 DUO 2.1GHz
Memory：	1.47GB
OS：	Microsoft Windows XP Professional SP3
Java ランタイムパラメータ：	最大ヒープサイズ 256MB (-Xmx256m)

- 解析時間

Apache-5：34 分

Apache-6：44 分

※各自の動作させる環境によって時間の差異は発生します。ご了承下さい。

4.20. 実行中、「入力ファイルに必須のカラムデータが存在していません。」という旨のメッセージが表示され、処理が中止されました。どうすればよいですか？

Web サーバのアクセスログかどうか今一度ご確認をお願いいたします。また、アクセスログのログタイプが異なるか、必須項目が出力されていない可能性もありますので、ログの項目の確認をお願いいたします。アクセスログについての詳細は、「解析対象のアクセスログ詳細」をご確認ください。

4.21. 今回のバージョンアップで追加した機能は何ですか。

今回のバージョンアップで追加した機能の内容は以下の通りです。

1. より多くの脆弱性を検出できるようになりました。
   - SQL インジェクションの検出パターンを増加
   - OS コマンド・インジェクションを検出する処理を追加
   - ディレクトリ・トラバーサルを検出する処理を追加
   - クロスサイト・スクリプティングを検出する処理を追加

- その他（IDS[5]回避を目的とした攻撃）を検出する処理を追加

2. 解析対象アクセスログを増やしました。
   - IIS5.1/7.0 の W3C 拡張ログファイルタイプのアクセスログ解析処理の追加

3. 動作するプラットフォームを拡大しました。
   - Linux 系 OS 上での動作確認
   - 他、IE 以外のブラウザでの動作確認

[5] IDS : 侵入検知システム (Intrusion Detection System)

5. Tips 集

iLogScanner が公開されてからあった問合せのあったものや参考資料を Tips 集として記載しております。(2008 年 11 月現在)

5.1. VlineLinux4.2 + FireFox2.0 +JRE6 においての文字化け対応

VlineLinux4.2 + FireFox2.0 +JRE6 の動作環境において、Java アプレットの日本語表示で英数字以外の文字が全て"□"で表示されてしまう現象の対応方法について、以下に文字化けが解消した事例を記載します。

１．ディレクトリ作成
　# mkdir /usr/java/jrexxxxx/lib/fonts/fallback
２．ディレクトリ移動して
　# cd /usr/java/jrexxxxx/lib/fonts/fallback
３．フォントのシンボリックリンクを張る
　# ln -s /usr/share/fonts/alias/TrueType/*.ttf .
４．Firefox を再起動

参考 URL：http://java.sun.com/j2se/1.5.0/ja/relnotes.html#linux

5.2. IIS7.0 での W3C フィールとの設定方法について

IIS6.0 までと IIS7.0 以降で設定方法が変わります。IIS7.0 の設定方法ですが、マイクロソフトの技術情報サイトに詳細な設定方法が記述されています。以下に URL を記載しますのでそちらの情報を参考にしてください。

URL：	http://www.microsoft.com/japan/technet/windowsserver/2008/library/d0de9475-0439-4ec1-8337-2bcedacd15c7.mspx?mfr=true

SQL インジェクション検出ツール「iLogScanner」取扱説明書

－ウェブサーバのアクセスログを解析して脆弱性を狙った攻撃の検出を簡易に行うツール－

［　発　行　］２００８年　４月１８日 iLogScanner V1.0 版
　　　　　　　２００８年１１月１１日 iLogScanner V2.0 版
［　発行者　］独立行政法人 情報処理推進機構 セキュリティセンター